

Reporte ejecutivo: Incidente de Ciberseguridad en web de Sanborns Mexico

Qué ocurrió

Alrededor del 25 de enero de 2026, se identificó un incidente de ciberseguridad en el portal oficial sanborns.com.mx, donde un actor de amenazas que utiliza el alias @h4ckzu5 logró acceso no autorizado al servidor web.

Cómo ocurrió

El ataque fue clasificado como un defacement ligero es decir modifica el contenido visible de un sitio web sin autorización, en la cual el atacante no compromete totalmente la funcionalidad del sitio, sino que deja evidencia de la intrusión. Como prueba, se detectó un archivo .txt alojado directamente en el servidor, lo que confirma que el atacante contó con privilegios de escritura, evidenciando fallas en los controles de acceso.

Quién lo confirmó

Especialistas en ciberseguridad de TPX Security, mediante publicaciones en la red social X, confirmaron la exposición del entorno web y la veracidad del hallazgo.

Gravedad

El nivel de gravedad se considera moderado. Hasta el momento, no existe confirmación de la extracción masiva de datos personales o financieros; sin embargo, el acceso no autorizado representa un riesgo potencial para la información de los usuarios y la integridad del sistema.

Contexto

El incidente se presenta en un periodo de alta actividad de ciberataques en México durante enero de 2026, afectando a diversas empresas y entidades relacionadas con grandes consorcios comerciales.

Evidencia



← يسوع الشيطان
723 posts



يسوع الشيطان
@h4ckzu5

h4ckzu5@mail2tor.co
qTox ID:
4E941CF33C516E8D32C0016FDBD78DDF529F5A89916C27DB735807365EF3B5
065626E415F615
Mis Certificaciones:
OSEP, OSIR, OSWE y OSCP+

📍 Todo el mundo ... 🔗 ...t4kyfgzwuczd457w5ehfgbssbeazsad.onion
📅 Joined March 2011 >

139 Following 879 Followers

Not followed by anyone you're following